IMPROVEMENTS IN AND RELATING TO DATA PROCESSING APPARATUS AND VERIFICATION METHODS

Field of the Invention

The present invention relates to data processing apparatus and to verification methods.

Background to the Invention

Despite the growing proliferation of computer hardware and software, there are still serious problems associated with data entry, and with the security of both hardware and software. Many new problems have arisen and others have become exacerbated as more and more computers are networked together and linked to the internet. One particular problem is that of remote hacking in which an unauthorised user seeks access to a computer or computer network by accessing the computer or a computer on the network otherwise than though a local keyboard or other local peripheral input device.

The present invention aims to provide in preferred embodiments thereof, data processing apparatus and verification methods that address at least one of these problems.

Summary of the Invention

According to the present invention in a first aspect, there is provided in a data processing apparatus comprising a first input channel and a second input channel each for inputting signals, a security device for verifying a

password, and means for determining whether the password input to the security device comes from the second input channel, in which the security device will verify a correct password from the first input channel, but not from the second input channel, in which the security device is configured to receive signals from the first input channel and configured not to receive signals from the second input channel.

In this way, the device determines whether the password input thereto comes from the second input channel, ie it physically cannot come from this channel.

Suitably, the device receives signals only from the first input channel. Suitably, the device cannot receive signals from the second input channel.

Suitably, the apparatus further comprises means to determine whether the security device has verified the password and, if not, to vary operation of the apparatus. Normally, the variation will be a restriction in operation, typically it will render the apparatus unusable.

Suitably, the first input channel comprises a first peripheral input device. Suitably, the first peripheral input device comprises a keyboard and the security device is located to receive signals from the keyboard and transmit them to a keyboard controller or to a bus. Suitably, the device is located between the keyboard controller and the keyboard bus. Here, "between" is in the electronic sense, ie receives output from the keyboard controller and generates an input for the keyboard bus.

The device thus acts as an interface between the keyboard controller and the bus.

Suitably, the apparatus further comprises a control unit (such as a CPU) which interrogates the security device to determine whether a correct password has been entered. A password protected operation is performed only if the control unit receives such verification.

Suitably, the device encrypts all signals it receives. Suitably, a decryption tool is provided between the output of the device and the application to which they key presses comprise instructions.

According to the present invention in a second aspect, there is provided a method of verifying which of a first input channel and a second input channel is used in data processing apparatus, the method comprising the steps of upon input of a password to the apparatus, a security device receiving input from the first input channel not from the second input channel declining password authorisation, if the input is through the second input channel, and if the correct password is input through the first input channel providing a password verification.

Suitably, the method includes the step of determining whether the security device has verified the password and, if not, varying the operation of the apparatus. Normally, the variation will be a restriction in operation. Typically, it will render the apparatus unusable.

Suitably, a control unit (such as a CPU) interrogates the security device to determine whether the correct password has been entered.

Suitably, the method includes the step of receiving signals only from the first input channel. Suitably, the data processing apparatus includes a device for receiving signals. Suitably, the device cannot receive signals from the second input channel.

Suitably, the first input channel comprises a first peripheral input device. Suitably, the first peripheral input device comprises a keyboard and the security device is located to receive signals from the keyboard and transmit them to a keyboard controller or to a bus. Suitably, the device is located between the keyboard controller and the keyboard bus. Here, "between" is in the electronic sense, ie receives output from the keyboard controller and generates an input for the keyboard bus. The device thus acts as an interface between the keyboard controller and the bus.

Suitably, the apparatus further comprises a control unit (such as a CPU) which interrogates the security device to determine whether a correct password has been entered. A password protected operation is performed only if the control unit receives such verification.

Brief Description of the Figure

The present invention will now be described, by way of example only, with reference to the Figure that follows

which is a schematic illustration of an electronic data processing apparatus embodying the present invention.

Description of the Preferred Embodiments

In one preferred embodiment of the present invention, there is provided an electronic data processing apparatus, typically a personal computer ("PC") 2. The PC 2 receives input signals from peripheral input devices (eg keyboard, data socket, pen, voice recognition microphone etc). The PC includes a keyboard 4 having an associated bus 6 and a keyboard controller 8 forming a first input channel from the keyboard 4. The PC 2 also has at least one further input channel 10 for signals corresponding to those from the keyboard 4. Typically, this further input channel 10 will comprise a data socket for receipt of digital signals transmitted from a remote modem (not shown). The PC 2 generally treats signals received via the data socket in the same way as those received from the keyboard 4, except as set out below.

A security device 12 is located between the keyboard controller 8 and the bus 6. That is, the security device 12 is located to receive signals from the first input channel (the keyboard 4), but not from the further input channel (the data socket 10). The security device 12 has the following characteristics.

(i) It includes a fast and reversible encryption/decryption algorithm such as DES or T-code.

(ii) It has a volatile memory Random Access Memory (RAM) including authorisation codes or an algorithm therefor, or pre-stored password and means for checking whether an input password or code matches such an authorisation code or password.

(iii) It includes a real-time clock powered by a power supply.

The security device 12 is typically embodied in a board (not shown) including a microprocessor. The board may be integral to the PC 2 or be a separate plug-in board.

The security device 12 requires a password to be input to pass keyboard signals to the bus 8. If the password is not provided on demand (a limited number of tries may be permitted before a lock-out) the security device 12 will either block signals or vary them, for instance by encryption, to be unusable. The security device 12 is configured so that upon receipt of the correct password it is activated for a predetermined period of time, according to the in-built real-time clock. The period of time can be varied based upon the password or other authorisation received. While activated, the security device 12 transmits keyboard signals unaltered. When not activated it is in the encryption state and encrypts signals passing therethrough (or may block them). Thus, while in the encryption state the central processing unit ("CPU") of PC 2 cannot understand the output of keyboard 8.

The security device 12 when activated and authorised receives input signals from the keyboard bus and outputs

them to the keyboard controller. The delay is insignificant.

In use, the PC 2 is configured to require a password before permitting access to certain functions or data (which may be all functions and/or data). By way of example, a word-processing file may be password protected. Before permitting access to the file, the PC CPU requires confirmation from the security device 12 that the correct password has been entered. Only if the CPU receives verification from the security device that the correct password has been entered will it perform the password protected operation. Since the security device 12 can only receive inputs from the keyboard, it is not possible to enter the password from any other source.

In this way, it is possible to verify the physical presence of a user. If signals are input to the PC via a modem, for instance from a "hacker", it will not be received via the keyboard input channel and so the password cannot be verified. Thus access can be denied to remote users or additional security measures put in place before allowing them access.

Typically, data will be encrypted and decryption will only be permitted upon verification from the security device 12.

Preferred embodiments of the present invention also enable a security enhancement to be provided to prevent "key logging" attacks. This is where a hacker loads a short application on to a PC to be attached which application interrogates the operating system to determine

each keystroke as it is pressed. A record of keystrokes can be used to inspect confidential information and/or retrieve passwords.

To prevent this the security device 12 can be set to encrypt all key presses according to a predetermined encryption algorithm. An encryption algorithm is used to ensure that generally a given key press when repeated does not generate as an output from the security device 12 the same output. A tool is additionally provided between the operating system and the application to be controlled by the key presses to decrypt the encrypted key press data. Therefore since the key press information available to the operating system is encrypted it is of no use to a key logger.

Although reference is made herein to a "password", that can comprise any signal or combination of signals and need not be a "word" at all.

Clearly, in certain embodiments the apparatus may only verify input from other inputs, usually being peripheral input devices.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings),

and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.